OFFICE OF THE UNDER SECRETARY OF DEFENSE

WASHINGTON, D.C. 20301-2000

POLICY

4 August 1989

Mr. Jack Wright
Information Privacy Coordinator
ATTN: [redacted] STAT
Central Intelligence Agency
Washington, D.C 20505

Dear Mr. Wright:

Reference is made to the telephone conversation today between [redacted] of your staff and Mr. Fred Cook of this office. STAT

We have asked Department of Defense Components and the Information Security Oversight Office (ISOO) to review the enclosed DoD Directive 5200.30, "Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records," for currency and completeness.

Because enclosure 6 of the Directive deals with guidelines for systematic declassification review of areas of interest to the Central Intelligence Agency, it is requested that this enclosure be reviewed. Please advise us of the results of your review at your earliest convenience.

My point of contact is Mr. Fred Cook, telephone 695-2289/2686.

Sincerely,

Richard K. Williams

Arthur E. Fajans
Director
Security Plans and Programs

Enclosure
As stated

cc: (w/o encl)
Director, ISOO
Chief, Records Declassification Division
National Archives and Records Administration

March 21, 1983
NUMBER 5200.30

Department of Defense Directive USD(P)

SUBJECT: Guidelines for Systematic Declassification Review of Classified Information in Permanently Valuable DoD Records

References: (a) DoD Directive 5200.30, "Guidelines for Systematic Review of 20-Year-Old Classified Information in Permanently Valuable DoD Records," September 9, 1981 (hereby canceled)
(b) Executive Order 12356, "National Security Information," April 2, 1982
(c) Information Security Oversight Office Directive No. 1 Concerning National Security Information, June 23, 1982
(d) through (g), see enclosure 1

A. REISSUANCE AND PURPOSE

This Directive reissues reference (a); establishes procedures and assigns responsibilities for the systematic declassification review of information classified under references (b) and (c), DoD Directive 5200.1 and DoD 5200.1-R (references (d) and (e)), and prior orders, directives, and regulations governing security classification; and implements section 3.3 of reference (b).

B. APPLICABILITY AND SCOPE

1. This Directive applies to the Office of the Secretary of Defense (OSD) and to activities assigned to the OSD for administrative support, the Military Departments, the Organization of the Joint Chiefs of Staff, the Unified and Specified Commands, and the Defense Agencies (hereafter referred to collectively as "DoD Components").

2. This Directive applies to the systematic review of permanently valuable classified information, developed by or for the Department of Defense and its Components, or its predecessor components and activities, that is under the exclusive or final original classification jurisdiction of the Department of Defense.

3. Its provisions do not cover Restricted Data or Formerly Restricted Data under the Atomic Energy Act of 1954 (reference (f)) or information in nonpermanent records.

4. Systematic declassification review of records pertaining to intelligence activities (including special activities) or intelligence sources or methods shall be in accordance with special procedures issued by the Director of Central Intelligence.

4. Systematic review for declassification shall be in accordance with procedures contained in DoD 5200.1-R (reference (e)). Information that falls within any of the categories in enclosures 2 and 3 shall be declassified if the designated DoD reviewer determines, in light of the declassification considerations contained in enclosure 4, that classification no longer is required. In the absence of such a declassification determination, the classification of the information shall continue as long as required by national security considerations.

5. Before any declassification or downgrading action, DoD information under review should be coordinated with the Department of State on subjects cited in enclosure 5, and with the Central Intelligence Agency (CIA) on subjects cited in enclosure 6.

F. RESPONSIBILITIES

1. The Deputy Under Secretary of Defense for Policy shall:

a. Exercise oversight and policy supervision over the implementation of this Directive.

b. Request DoD Components to review enclosures 2 and 4 of this Directive every 5 years.

c. Revise enclosures 2 and 4 to ensure they meet DoD needs.

d. Authorize, when appropriate, other federal agencies to apply this Directive to DoD information in their possession.

2. The Head of each DoD Component shall:

a. Recommend changes to the enclosures of this Directive.

b. Propose, with respect to specific programs, projects, and systems under his or her classification jurisdiction, supplements to enclosures 2 and 4 of this Directive.

c. Provide advice and designate experienced personnel to provide timely assistance to the Archivist of the United States in the systematic review of records under this Directive.

3. The Director, National Security Agency/Chief, Central Security Service (NSA/CSS), shall develop, for approval by the Secretary of Defense, special procedures for systematic review and declassification of classified cryptologic information.

4. The Archivist of the United States is authorized to apply this Directive when reviewing DoD classified information that has been accessioned into the Archives of the United States.

REFERENCES, continued

(d) DoD Directive 5200.1, "DoD Information Security Program," June 7, 1982
(e) DoD 5200.1-R, "Information Security Program Regulation," August 1982, authorized by DoD Directive 5200.1, June 7, 1982
(f) Public Law 83-703, Atomic Energy Act of 1954
(g) Title 44, United States Code, Section 2103

CATEGORIES OF INFORMATION THAT REQUIRE REVIEW BEFORE DECLASSIFICATION

The following categories of information shall be reviewed systematically for declassification by designated DoD reviewers in accordance with this Directive:

1. Nuclear propulsion information.

2. Information concerning the establishment, operation, and support of the U.S. Atomic Energy Detection System.

3. Information concerning the safeguarding of nuclear materials or facilities.

4. Information that could affect the conduct of current or future U.S. foreign relations. (Also see enclosure 5.)

5. Information that could affect the current or future military usefulness of policies, programs, weapon systems, operations, or plans when such information would reveal courses of action, concepts, tactics, or techniques that are used in current operations plans.

6. Research, development, test, and evaluation (RDT&E) of chemical and biological weapons and defensive systems; specific identification of chemical and biological agents and munitions; chemical and biological warfare plans; and U.S. vulnerability to chemical or biological warfare attack.

7. Information about capabilities, installations, exercises, research, development, testing and evaluation, plans, operations, procedures, techniques, organization, training, sensitive liaison and relationships, and equipment concerning psychological operations; escape, evasion, rescue and recovery, insertion, and infiltration and exfiltration; cover and support; deception; unconventional warfare and special operations; and the personnel assigned to or engaged in these activities.

8. Information that reveals sources or methods of intelligence or counterintelligence, counterintelligence activities, special activities, identities of clandestine human agents, methods of special operations, analytical techniques for the interpretation of intelligence data, and foreign intelligence reporting. This includes information that reveals the overall scope, processing rates, timeliness, and accuracy of intelligence systems and networks, including the means of interconnecting such systems and networks and their vulnerabilities.

9. Information that relates to intelligence activities conducted jointly by the Department of Defense with other federal agencies or to intelligence activities conducted by other federal agencies in which the Department of Defense has provided support. (Also see enclosure 6.)

10. Airborne radar and infrared imagery.

11. Information that reveals space system:

a. Design features, capabilities, and limitations (such as antijam characteristics, physical survivability features, command and control design details, design vulnerabilities, or vital parameters)

(2) Those that relate to SIGINT. These appear as reports in various formats that bear security classifications, sometimes followed by five-letter codewords (World War II's ULTRA, for example) and often carrying warning caveats such as "This document contains codeword material" and "Utmost secrecy is necessary..." Formats may appear as messages having addressees, "from" and "to" sections, and as summaries with SIGINT content with or without other kinds of intelligence and comment.

(3) RDT&E reports and information that relate to either COMSEC or SIGINT.

b. Commonly used words that may help in identification of cryptologic documents and materials are "cipher," "code," "codeword," "communications intelligence" or "COMINT," "communications security" or "COMSEC," "cryptanalysis," "crypto," "cryptography," "cryptosystem," "decipher," "decode," "decrypt," "direction finding," "electronic intelligence" or "ELINT," "electronic security," "encipher," "encode," "encrypt," "intercept," "key book," "signals intelligence" or "SIGINT," "signal security," and "TEMPEST."

Attachments - 3
1. Department of the Army Systems
2. Department of the Navy Systems
3. Department of the Air Force Systems

CATEGORIES OF INFORMATION THAT REQUIRE REVIEW BEFORE DECLASSIFICATION
DEPARTMENT OF THE ARMY SYSTEMS

The following categories of Army information shall be reviewed systematically for declassification by designated DoD reviewers in accordance with this Directive.

1. Ballistic Missile Defense (BMD) missile information, including the principle of operation of warheads (fuzing, arming, firing, and destruct operations); quality or reliability requirements; threat data; vulnerability; ECM and ECCM; details of design, assembly, and construction; and principle of operations.

2. BMD systems data, including the concept definition (tentative roles, threat definition, and analysis and effectiveness); detailed quantitative technical system description-revealing capabilities or unique weaknesses that are exploitable; overall assessment of specific threat-revealing vulnerability or capability; discrimination technology; and details of operational concepts.

3. BMD optics information that may provide signature characteristics of U.S. and United Kingdom ballistic weapons.

4. Shaped-charge technology.

5. Fleshettes.

6. M380 Beehive round.

7. Electromagnetic propulsion technology.

8. Space weapons concepts.

9. Radar-fuzing programs.

10. Guided projectiles technology.

11. ECM and ECCM to weapons systems.

12. Armor materials concepts, designs, or research.

13. 2.75-inch Rocket System.

14. Air Defense Command and Coordination System (AN/TSQ-51).

15. Airborne Target Acquisition and Fire Control System.

16. Chaparral Missile System.

17. Dragon Guided Missile System Surface Attack, M47.

18. Forward Area Alerting Radar (FAAR) System.

CATEGORIES OF INFORMATION THAT REQUIRE REVIEW BEFORE DECLASSIFICATION
DEPARTMENT OF THE NAVY SYSTEMS

The following categories of Navy information shall be reviewed systematically for declassification by designated DoD reviewers in accordance with this Directive.

1. Naval nuclear propulsion information.

2. Conventional surface ship information:

a. Vulnerabilities of protective systems, specifically:

(1) Passive protection information concerning ballistic torpedo and underbottom protective systems.

(2) Weapon protection requirement levels for conventional, nuclear, biological, or chemical weapons.

(3) General arrangements, drawings, and booklets of general plans (applicable to carriers only).

b. Ship-silencing information relative to:

(1) Signatures (acoustic, seismic, infrared, magnetic (including alternating magnetic (AM)), pressure, and underwater electric potential (UEP)).

(2) Procedures and techniques for noise reduction pertaining to an individual ship's component.

(3) Vibration data relating to hull and machinery.

c. Operational characteristics related to performance as follows:

(1) Endurance or total fuel capacity.

(2) Tactical information, such as times for ship turning, zero to maximum speed, and maximum to zero speed.

3. All information that is uniquely applicable to nuclear-powered surface ships or submarines.

4. Information concerning diesel submarines as follows:

a. Ship-silencing data or acoustic warfare systems relative to:

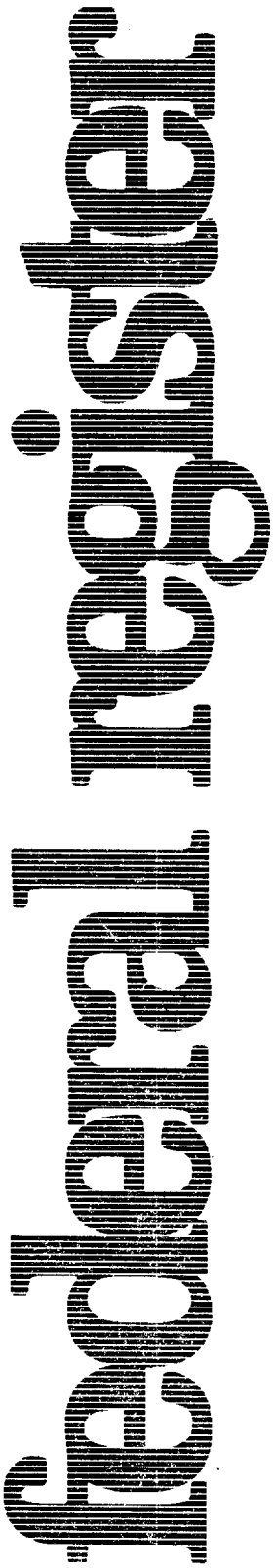
(1) Overside, platform, and sonar noise signature.

(2) Radiated noise and echo response.

(3) All vibration data.

CATEGORIES OF INFORMATION THAT REQUIRE REVIEW BEFORE DECLASSIFICATION
DEPARTMENT OF THE AIR FORCE SYSTEMS

The Department of the Air Force has determined that the categories identified in enclosure 2 of this Directive shall apply to Air Force information.



Monday
January 31, 1983

Part III

Information Security Oversight Office

National Security Information; General Guidelines for Systematic Declassification Review of Foreign Government Information; Final Rule

(d) Foreign government information falling within any of the categories listed in § 2002.6 of these guidelines shall be declassified or downgraded only upon specific authorization of the agency that has declassification authority over it. Such information shall be referred to the responsible agency(ies) for review. Information so referred shall remain classified until the responsible agency(ies) has declassified it. If the responsible agency cannot be readily identified from the document or material, referral shall be made in accordance with § 2002.7 of these guidelines.

(e) When required, the agency having declassification authority over the information shall consult with foreign governments concerning its proposed declassification.

§ 2002.5 Effect of publication.

(a) Foreign government information shall be considered declassified when published in an unclassified United States Government executive branch publication (e.g., the *Foreign Relations of the United States* series) or when cleared for publication by United States Government executive branch officials authorized to declassify the information; or if officially published as unclassified by the foreign government(s) or international organization(s) of governments that furnished the information unless the fact of the U.S. Government's possession of the information requires continued protection.

(b) The unofficial publication, in the United States or abroad, of foreign government information contained in classified United States or foreign documents does not in or of itself constitute or permit the declassification of such information. Although prior unofficial publication is a factor to be considered in the systematic review process, there may be valid reasons for continued protection of the information which could preclude its declassification. In particular, the classification status of foreign government information which concerns or derives from intelligence activities (including special activities), intelligence sources or methods shall not be affected by any unofficial publication of identical or related information. The final declassification determination shall be made by the agency or agencies having declassification authority over it.

§ 2002.6 Categories requiring item-by-item review.

Foreign government information falling into the following categories require item-by-item review for declassification by agencies having declassification authority over it.

(a) Information exempted from declassification under any joint arrangement evidenced by an exchange of letters, memorandum of understanding, or other written record, with the foreign government or international organization of governments, or element(s) thereof, that furnished the information. Questions concerning the existence or applicability of such arrangements shall be referred to the agency or agencies having declassification authority over the records under review.

(b) Information related to the safeguarding of nuclear materials or facilities, foreign and domestic, including but not necessarily limited to vulnerabilities and vulnerability assessments of nuclear facilities and Special Nuclear Material.

(c) Nuclear arms control information (see also paragraph (k) of this section).

(d) Information regarding foreign nuclear programs (other than "Restricted Data" and "Formerly Restricted Data"), such as:

(1) Nuclear weapons testing.

(2) Nuclear weapons storage and stockpile.

(3) Nuclear weapons effects, hardness, and vulnerability.

(4) Nuclear weapons safety.

(5) Cooperation in nuclear programs including, but not limited to, peaceful and military applications of nuclear energy.

(6) Exploration, production and import of uranium and thorium from foreign countries.

(e) Information concerning intelligence activities (including special activities) or intelligence or counterintelligence sources or methods including but not limited to intelligence, counterintelligence and covert action programs, plans, policies, operations, or assessments; or which would reveal or identify:

(1) Any present, past or prospective undercover personnel, installation, unit, or clandestine human agent, of the United States or a foreign government;

(2) Any present, past or prospective method, procedure, mode, technique or requirement used or being developed by the United States or by foreign governments, individually or in combination to produce, acquire, transmit, analyze, correlate, assess, evaluate or process intelligence or counterintelligence, or to support an intelligence or counterintelligence source, operation, or activity;

(3) The present, past or proposed existence of any joint United States and foreign government intelligence, counterintelligence, or covert action activity or facility, or the nature thereof. (For guidance on protecting United States foreign intelligence liaison relationships, see Director of Central Intelligence Directive "Security Classification Guidance and Foreign Security Services," effective January 18, 1982.)

(f) Information that could result in or lead to actions which would place an individual in jeopardy attributable to disclosure of the information, including but not limited to:

(1) Information identifying any individual or organization as a confidential source of intelligence or counterintelligence.

(2) Information revealing the identity of an intelligence or covert action agent or agents.

(3) Information identifying any individual or organization used to develop or support intelligence, counterintelligence, or covert action agents, sources or activities.

(g) Information about foreign individuals, organizations or events which if disclosed, could be expected to:

(1) Adversely affect a foreign country's or international organization's present or future relations with the United States.

(2) Adversely affect present or future confidential exchanges beween the United States and any foreign government or international organization of governments.

(h) Information related to plans (whether executed or not, whether presented in whole or in part), programs, operations, negotiations, and assessments shared by one or several foreign governments with the United States, including but not limited to those involving the territory, political regime or government of another country, and which if disclosed could be expected to adversely affect the conduct of U.S. foreign policy or the conduct of another country's foreign policy with respect to a third country or countries. This item would include contigency plans, plans for covert political, military or paramilitary activities or operations by a foreign government acting alone or jointly with the United States Government, and positions or actions taken by a foreign government alone or jointly with the United States concerning border disputes or other territorial issues.

(i) Information concerning arrangements with respect to foreign basing of cryptologic operations and/or foreign policy considerations relating thereto.

§ 2002.8 Downgrading.

Foreign government information classified "Top Secret" may be downgraded to "Secret" after 30 years unless the agency with declassification authority over it determines on its own, or after consultation, as appropriate, with the foreign government or international organization of governments which furnished the information, that it requires continued protection at the "Top Secret" level.

Dated: January 27, 1983.

Steven Garfinkel,

Director, Information Security Oversight Office.

[FR Doc. 83-2614 Filed 1-28-83; 8:45 am]
BILLING CODE 6820-AF-M

DECLASSIFICATION CONSIDERATIONS

1. Technological developments; widespread public knowledge of the subject matter; changes in military plans, operations, systems, or equipment; changes in the foreign relations or defense commitments of the United States; and similar events may bear upon the determination of whether information should be declassified. If the responsible DoD reviewer decides that, in view of such circumstances, the public disclosure of the information being reviewed no longer would result in damage to the national security, the information shall be declassified.

2. The following are examples of considerations that may be appropriate in deciding whether information in the categories listed in enclosure 2 may be declassified when it is reviewed:

a. The information no longer provides the United States a scientific, engineering, technical, operational, intelligence, strategic, or tactical advantage over other nations.

b. The operational military capability of the United States revealed by the information no longer constitutes a limitation on the effectiveness of the Armed Forces.

c. The information is pertinent to a system that no longer is used or relied on for the defense of the United States or its allies and does not disclose the capabilities or vulnerabilities of existing operational systems.

d. The program, project, or system information no longer reveals a current weakness or vulnerability.

e. The information pertains to an intelligence objective or diplomatic initiative that has been abandoned or achieved and will no longer damage the foreign relations of the United States.

f. The information reveals the fact or identity of a U.S. intelligence source, method, or capability that no longer is employed and that relates to no current source, method, or capability that upon disclosure could cause damage to national security or place a person in immediate jeopardy.

g. The information concerns foreign relations matters whose disclosure can no longer be expected to cause or increase international tension to the detriment of the national security of the United States.

3. Declassification of information that reveals the identities of clandestine human agents shall be accomplished only in accordance with procedures established by the Director of Central Intelligence for that purpose.

4. The NSA/CSS is the sole authority for the review and declassification of classified cryptologic information. The procedures established by the NSA/CSS to facilitate the review and declassification of classified cryptologic information are:

DEPARTMENT OF STATE AREAS OF INTEREST

1. Statements of U.S. intent to defend, or not to defend, identifiable areas, or along identifiable lines, in any foreign country or region.

2. Statements of U.S. intent militarily to attack in stated contingencies identifiable areas in any foreign country or region.

3. Statements of U.S. policies or initiatives within collective security organizations (for example, North Atlantic Treaty Organization (NATO) and Organization of American States (OAS)).

4. Agreements with foreign countries for the use of, or access to, military facilities.

5. Contingency plans insofar as they involve other countries, the use of foreign bases, territory or airspace, or the use of chemical, biological, or nuclear weapons.

6. Defense surveys of foreign territories for purposes of basing or use in contingencies.

7. Reports documenting conversations with foreign officials, that is, foreign government information.

CENTRAL INTELLIGENCE AGENCY AREAS OF INTEREST

1. Cryptologic, cryptographic, or SIGINT. (Information in this category shall continue to be forwarded to the NSA/CSS in accordance with enclosure 4, paragraph 4. The NSA/CSS shall arrange for necessary coordination.)

2. Counterintelligence.

3. Special access programs.

4. Information that identifies clandestine organizations, agents, sources, or methods.

5. Information on personnel under official or nonofficial cover or revelation of a cover arrangement.

6. Covertly obtained intelligence reports and the derivative information that would divulge intelligence sources or methods.

7. Methods or procedures used to acquire, produce, or support intelligence activities.

8. CIA structure, size, installations, security, objectives, and budget.

9. Information that would divulge intelligence interests, value, or extent of knowledge on a subject.

10. Training provided to or by the CIA that would indicate its capability or identify personnel.

11. Personnel recruiting, hiring, training, assignment, and evaluation policies.

12. Information that could lead to foreign political, economic, or military action against the United States or its allies.

13. Events leading to international tension that would affect U.S. foreign policy.

14. Diplomatic or economic activities affecting national security or international security negotiations.

15. Information affecting U.S. plans to meet diplomatic contingencies affecting national security.

16. Nonattributable activities conducted abroad in support of U.S. foreign policy.

17. U.S. surreptitious collection in a foreign nation that would affect relations with the country.

18. Covert relationships with international organizations or foreign governments.

Next 1 Page(s) In Document Denied